IN THE CLAIMS:

Pending claims follow:

1. (Previously Amended) A method for on-access computer virus scanning of files in an efficient manner, comprising:

(a) identifying a process for accessing files;

(b) selecting virus detection actions based at least in part on the process; and

(c) performing the virus detection actions on the files;

wherein the process is identified from a plurality of processes each carried out by an executable file, the processes including at least one process initiated by an application program selected from the group consisting of a network browser application and a word processor application, for tailoring the virus detection actions when the application program attempts to access the files.

2. (Cancelled)

3. (Original) The method as recited in claim 1, wherein the virus detection actions are selected by determining a category associated with the process, and selecting a set of virus detection actions based on the determined category.

4. (Original) The method as recited in claim 1, and further comprising the steps of identifying the files being accessed, and selecting the virus detection actions based at least in part on the identity of the files.

5. (Original) The method as recited in claim 1, wherein the process is identified by inspecting at least one of a name of the process, a path of the process, a file signature associated with the process, a version of the process, a manufacturer of the process, a function being called during the process, an

owner of the process, a name of an executable file associated with the process, a method in which files are being accessed by the process, type(s) of shared libraries used by the identified process, and a user of the process.

6. (Original) The method as recited in claim 1, wherein no virus detection actions are selected upon the identification of a predetermined process.

7. (Previously Amended) A computer program product embodied on a computer readable medium for on-access computer virus scanning of files in an efficient manner, comprising:

(a) computer code for identifying a process for accessing files;

(b) computer code for selecting virus detection actions based at least in part on the process; and

(c) computer code for performing the virus detection actions on the files;

wherein the process is identified from a plurality of processes each carried out by an executable file, the processes including at least one process initiated by an application program selected from the group consisting of a network browser application and a word processor application, for tailoring the virus detection actions when the application program attempts to access the files.

8. (Cancelled)

9. (Original) The computer program product as recited in claim 7, wherein the virus detection actions are selected by determining a category associated with the process, and selecting a set of virus detection actions based on the determined category.

10. (Original) The computer program product as recited in claim 7, and further comprising computer code for identifying the files being accessed, and selecting the virus detection actions based at least in part on the identity of the files.

11. (Original) The computer program product as recited in claim 7, wherein the process is identified by inspecting at least one of a name of the process, a path of the process, a file signature associated with the process, a version of the process, a manufacturer of the process, a function being called during the process, an owner of the process, a name of an executable file associated with the process, a method in which files are being accessed by the process, type(s) of shared libraries used by the process, and a user of the process.

12. (Original) The computer program product as recited in claim 7, wherein no virus detection actions are selected upon the identification of a predetermined process.

13. (Previously Amended) A system for on-access computer virus scanning of files in an efficient manner, comprising:

(a) logic for identifying a process for accessing files;

(b) logic for selecting virus detection actions based at least in part on the process; and

(c) logic for performing the virus detection actions on the files;

wherein the process is identified from a plurality of processes each carried out by an executable file, the processes including at least one process initiated by an application program selected from the group consisting of a network browser application and a word processor application, for tailoring the virus detection actions when the application program attempts to access the files.

14. (Cancelled)

15. (Original) The system as recited in claim 13, wherein the virus detection actions are selected by determining a category associated with the process, and selecting a set of virus detection actions based on the determined category.

16. (Original) The system as recited in claim 13, and further comprising logic for identifying the files being accessed, and selecting the virus detection actions based at least in part on the identity of the files.

17. (Original) The system as recited in claim 13, wherein the process is identified by inspecting at least one of a name of the process, a path of the process, a file signature associated with the process, a version of the process, a manufacturer of the process, a function being called during the process, an owner of the process, a name of an executable file associated with the process, a method in which files are being accessed by the process, type(s) of shared libraries used by the process, and a user of the process.

18. (Original) The system as recited in claim 13, wherein no virus detection actions are selected upon the identification of a predetermined process.

19. – 23. (Cancelled)

24. (Previously Amended) A method for computer virus scanning of files in an efficient manner, comprising:
defining a plurality of extensions indicative of different types of files based on a user;
identifying a file being accessed;
determining the extension of the file being accessed; and
performing virus detection actions on the file based on whether the extension is defined by the user;
wherein at least a portion of the extensions relates to a plurality of processes each carried out by an executable file, the processes including at least one process initiated by an application program selected from the group consisting of a network browser application and a word processor application, for tailoring the virus detection actions when the application program attempts to access the file.

25. (Previously Amended) A computer program product embodied on a computer readable medium for computer virus scanning of files in an efficient manner, comprising:

computer code for defining a plurality of extensions indicative of different types of files based on a user;

computer code for identifying a file being accessed;

computer code for determining the extension of the file being accessed; and

computer code for performing virus detection actions on the file based on whether the extension is defined by the user;

wherein at least a portion of the extensions relates to a plurality of processes each carried out by an executable file, the processes including at least one process initiated by an application program selected from the group consisting of a network browser application and a word processor application, for tailoring the virus detection actions when the application program attempts to access the file.

26. (Previously Amended) A method for computer virus scanning of files in an efficient manner, comprising:

identifying a file being accessed;

identifying a process for accessing the file;

determining a category associated with the process;

selecting a set of virus detection actions based on the determined category;

determining an extension of the file being accessed; and

performing the virus detection actions on the files based on the extension. ;

wherein the process is identified from a plurality of processes each carried out by an executable file, the processes including at least one process initiated by an application program selected from the group consisting of a network browser application and a word processor application, for tailoring the virus detection actions when the application program attempts to access the file.

27. (Previously Amended) A method for computer virus scanning of files in an efficient manner, comprising:

defining a plurality of extensions indicative of different types of files based on a user;

defining a plurality of categories indicative of different types of processes;

identifying a file being accessed;

identifying a process for accessing the file;
determining a category associated with the process;
selecting a set of virus detection actions based on the determined category;
determining the extension of the file being accessed; and
if the extension is defined by the user, performing the virus detection actions on the files;
wherein the process is identified from a plurality of processes each carried out by an executable file, the processes including at least one process initiated by an application program selected from the group consisting of a network browser application and a word processor application, for tailoring the virus detection actions when the application program attempts to access the files.

28. (Previously Amended) A method for on-access computer virus scanning of files in an efficient manner, comprising:
identifying a process for accessing files;
selecting virus detection actions based at least in part on the process; and
performing the virus detection actions on the files;
wherein downloading of infected files from the Internet is prevented;
wherein the process is identified from a plurality of processes each carried out by an executable file, the processes including at least one process initiated by an application program selected from the group consisting of a network browser application and a word processor application, for tailoring the virus detection actions when the application program attempts to access the files.

29. (Previously Presented) A method for on-access computer virus scanning of files in an efficient manner, comprising:
(a) identifying a process for accessing files;
(b) selecting virus detection actions based at least in part on the process; and
(c) performing the virus detection actions on the files;
wherein the process is identified from a plurality of processes each carried out by an executable file, the processes initiated by application program-related executable files including

FindFast.exe, WinWord.exe, and Explorer.exe, for tailoring the virus detection actions when attempts are made to access the files;

wherein the virus detection actions are selected by determining a category associated with the process, and selecting a set of virus detection actions based on the determined category;

wherein the process is identified by inspecting a name of the process, a path of the process, a file signature associated with the process, a version of the process, a manufacturer of the process, a function being called during the process, an owner of the process, a name of an executable file associated with the process, a method in which files are being accessed by the process, type(s) of shared libraries used by the identified process, and a user of the process.